DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 7: System Administrator, Network Administrator, and End-User Training

1. References:

a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

c. AR 380-67, Personnel Security Program, 9 September 1988.

d. DA PAM 25-IA, Information Assurance Implementation Guide, 26 May 2000, Sections 1-5, IA Structure, and 2-2, IA Training.

e. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

f. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

g. DoD Instruction 5200.4, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

h. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

i. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

2. Purpose:

a. The 4ID recognizes that technology is evolving at a rapid rate and understands the need for personnel to develop skills to keep pace with technology changes. Therefore, a training program must be developed which ensures that 4ID retains qualified staff to administer information systems and maintain an information assurance program.

b. Information Assurance training is an integral part of ensuring that 4ID resources are effectively secured and protected from internal and external breaches and exploitations.

c. This policy provides directives for the establishment and on-going involvement of an Information Assurance training program for 4ID network/systems administrators, end-users, and IA personnel.

d. 4ID designs, implements, operates, and maintains information technology and local and wide area communications infrastructure that supports numerous commands and thousands of end-users. Various Information Assurance personnel and network/systems administrators and managers are responsible for operating, maintaining, and safeguarding these information resources. It is crucial that these personnel are adept in the security measures and safeguards that must be used and implemented in order to provide for continuous protection of 4ID assets. The end-user community must also be aware of the various security vulnerabilities associated with automated information systems (AIS) and 4IDinformation resources. In order to sustain a steadfast security posture, end-users must know what

precautions to take, how to recognize possible exploits and breaches, and how they get reported.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

   a. Compliance with this policy is the responsibility of the respective organization commander\director.

   b. The 4ID Information Assurance Manager (IAM) shall centrally oversee and verify compliance with all 4ID IA training requirements for IA staff, network and systems administrators, and end-users.

   c. 4ID personnel are responsible for identifying opportunities and requesting approval for training from respective providers (e.g., SANS conference, Microsoft certification training, Cisco training, etc.) that would enhance their professional and technical qualifications and provide direct or ancillary benefit to their primary duties and responsibilities. Each individual must seek approval for such training through his or her normal chain of command. Individuals completing a training course must submit a notification of completed training to their IAM.

5. Policy:

   a. All network administrators, system administrators, network/system managers, and IA personnel, to include the Information Assurance Security Officer (IASO), Information Assurance Manager (IAM), Information Assurance Network Manager (IANM), and Systems Administrators (SA) shall undergo an Automated Information Systems (AIS) security course of instruction equal to the duties assigned to them and other requisite training as described in AR 25-2, paragraph 3-2.

   b. The instruction shall address: The scope and criticality of information assurance and security in today's information technology, Internet-connected environment, industry-practiced information security measures used to protect and secure an organization's information resources, techniques and methodologies used to educate the end-user community of the criticality of securing information assets, and techniques and methodologies used to enforce these information security measures.

   c. A record of completed training for IA personnel shall be maintained within the office of the respective IAM.

   d. The 4ID IAM shall oversee the development of an Information Security Awareness Training Module that is computer based and can be completed within 30 minutes by an end user with average IT skills. The security awareness program shall be maintained current and relevant as technology and security issues mature.

   e. All 4ID end-users shall undergo an initial security training and information assurance awareness briefing upon reporting to a 4ID facility. The briefing shall include the following:

      (1) Threats, vulnerabilities, and risks associated with the system. Under this portion, specific information regarding measures to reduce the threat from malicious software will be provided, including prohibitions on loading unauthorized software, the need for frequent backup, and the requirement to report abnormal program behavior immediately.

(2) Information security objectives (that is, what is it that needs to be protected?)

(3) Responsibilities and accountability associated with system security.

(4) Information accessibility, handling, and storage considerations.

(5) Physical and environmental considerations that are necessary to protect the system.

(6) System data and access controls.

(7) Emergency and disaster plans.

(8) Authorized system configuration and associated configuration management requirements.

f. Refresher training will be completed annually.

6. Non-Compliance: Each year a report shall be prepared listing those who participated in the Security Awareness training. That list shall be made available to 4ID Commanders for action by the chain of command to ensure that all personnel have received the requisite awareness training.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding